REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
03-05-2011	Master of Military Studies Research Paper	September 2010 - April 2011

4. TITLE AND SUBTITLE
CYBERSPACE: FREEDOM VS. SECURITY IN THE 21ST CENTURY

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Matthew J. Cutler, Major, USMC

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
N/A

12. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT
It is essential to balance internet freedom in cyberspace with security. The U.S. must protect its national interest and critical information in the cyber domain. Deterrence and defending U.S. critical information and infrastructure should be the Nation's primary focus in the cyber domain. Offensive actions should be limited and secretive in nature, with a great deal of plausible deniability. Kinetic responses to a cyber attack should only be conducted in times of war. Attributing responsibility to a sponsored state cyber attack from a non-state actor, such as a terrorist, is extremely difficult. The greatest deterrent to cyber attacks should be the international community – with an agreed-upon code of conduct between states.

15. SUBJECT TERMS
Cyberpsace, deterrence, cyber security, cyber threats, internet freedom.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	UU	29	Marine Corps University / Command and Staff College
Unclass	Unclass	Unclass			19b. TELEPONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at lest the year and be Year 2000 compliant, e.g., 30-06-1998; xx-08-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report, e.g. 1F665702D1257.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. AFOSR-82-1234.

5d. PROJECT NUMBER. Enter al project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORS AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

CYBERSPACE: FREEDOM VS. SECURITY IN THE 21ST CENTURY

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF MASTER OF
MILITARY STUDIES

MAJOR MATTHEW J. CUTLER

AY 10-11

Mentor and Oral Defense Committee Member: Eric Y. Shibuya, Ph.D., Associate Professor of Strategic Studies
Approved: [signature]
Date: 5 APRIL 2011

Oral Defense Committee Member: Jonathan E. Phillips
Approved: [signature]
Date: 5 April 2011

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENT AGENCY. REFERENCES TO THIS STUDY SHOULD INCLIDE THE FOREGOING STATEMENT.

Table of Contents

Executive Summary

Title: Cyberspace: Freedom vs. Security in the 21st Century

Author: Major Matthew J. Cutler, United States Marine Corps

Thesis: It is essential to balance internet freedom in cyberspace with security. The U.S. must protect its national interest and critical information, and deterrence and defending U.S. critical information and infrastructure should be the Nation's primary focus in the cyber domain. Offensive actions should be limited and secretive in nature, with a great deal of plausible deniability. Kinetic responses to a cyber attack should only be conducted in times of war. Attributing responsibility to a sponsored state cyber attack from a non-state actor, such as a terrorist, is extremely difficult. The greatest deterrent to cyber attacks should be the international community – with an agreed-upon code of conduct between states.

Discussion: Internet availability throughout the world is increasing, creating more free and open discussion and information-sharing unlike anything the world has seen before – globalization of information. The growing availability of these freedoms has positive and negative effects on the world in the 21st century. We have seen Hezbollah win a war strategically: rather than use overwhelming firepower or maneuverability, Hezbollah successfully utilized the internet to spread information and propaganda instantaneously with the world. Uprisings in the Middle East, from Tunisia to Yemen, have been begun not by a mission type order, but by social media outlets like Facebook. Cyber threats are real and pose a serious threat to our national interests both abroad and at home. Recent cyber attacks, such as the ones in Estonia, Georgia, and Iran, demonstrate the kind of power individuals, states and non-state actors can exert without firing a shot. Balancing internet freedoms with security will be an exceptional challenge for policy makers. If that were not hard enough, the real challenge in years to come lies in creating a deterrence agreement at an international level. While some fundamental approaches exist that can be used as guidelines, deterrence will only be achieved if the international community is serious about cyber security.

Conclusion: True deterrence must come with the cooperation of the international community. The structure of the NPT offers great insight on how to possibly achieve a cyber warfare international treaty, but the Bush doctrine offers up the best approach to combating cyber crimes. An international agreement on cyberspace security, with widely acceptable norms and procedures for cyber warfare, would deter cyber attacks, making them less tantalizing. Such an agreement would also create an incentive to preemptively detect, target, and neutralize non-state actors attempting to carry out attacks within a nation's territory. If the world is to truly balance internet freedom with security, such an agreement must exist.

Preface

I started this project wanting to write on something that was related to my job as a Marine communicator. I had just spent three years working at 1st Marine Aircraft Wing out in Okinawa and learned a great deal within my occupational specialty. Some of the things that I encountered were frustrating in allowing our staff to function properly with the abundant informational systems at their disposal. I thought we had not enabled them enough and created barriers at times. I understood the threats to our networks but I have always leaned towards enabling the users to complete their missions – timely and efficiently. To a great degree, I can relate to my title "Freedom Vs. Security." I lived it from a slightly different angle from what I discuss in this paper, but in all actuality, I think my experience drove me in this particular direction.

As I developed the initial draft of this paper, I found myself trying to connect two different but similar worlds. I thought I would be able to work off of my experiences primarily, but soon found that would not be possible. After doing research, mostly online and with current news, I was able to refine my paper. In the end, I think my topic is extremely relevant and is growing in popularity not only within the U.S. Government and Department of Defense, but with the common person throughout the world. I was able to learn a good deal regarding cyber security as I researched, finding it very interesting on the threats we face there and how deterrence will be a significant challenge when it comes to policymakers.

I would like to acknowledge my mentor in this process, Dr. Eric Shibuya. His direction and guidance were invaluable in development of this paper. I would especially like to thank my wife, Katie, and my two boys Jack and Logan for their support

throughout the process as well. Without them this would not have been possible – thank you.

Introduction

We are building the bridge to the future while standing on it.
- Anonymous[1]

The invention of the internet – and cyberspace – has changed the world dramatically in the last 15-20 years. Cyberspace is defined as, "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and imbedded processors and controllers."[2] In 1994, there were only around 500 websites worldwide.[3] Today, most recent data shows that there are over one trillion web pages in the world, and growing each day by the thousands.[4] This demonstrates that the internet has probably the fastest technological growth ever seen in the history of mankind. The ability for an individual to share information with anyone, anywhere, anytime has provided a desired freedom for people throughout the world – globalization of information. With this freedom comes a very daunting security concern for technologically advanced nations such as the United States.

Most of the Nation's critical infrastructure relies on cyberspace as the significant control system of the country – a kind of "nervous system" of the United States.[5] The U.S. military relies on cyberspace for the backbone of day-to-day battlefield operations at home and abroad. The U.S. faces two major concerns when it comes to cyberspace – freedom versus security. First, the U.S. wants to identify ways to utilize and maneuver in cyberspace to create an advantage, economically, diplomatically, militarily, and strategically. Secondly, and just as importantly, the U.S. needs to protect its information and critical nodes from a catastrophic cyber attack.

As cyberspace is beginning to define our culture, global society, and warfare in this century, how does the U.S. government defend against potentially devastating cyber attacks, and what kind of response is warranted? Will the U.S. treat cyber attacks by state and non-state actors differently? Finally, what is the best way to deter future cyber attacks?

It is essential to balance internet freedom in cyberspace with security. The U.S. must protect its national interest and critical information in the cyber domain. Deterrence and defending U.S. critical information and infrastructure should be the Nation's primary focus in the cyber domain. Offensive actions should be limited and secretive in nature, with a great deal of plausible deniability. Kinetic responses to a cyber attack should only be conducted in times of war. Attributing responsibility to a sponsored state cyber attack from a non-state actor, such as a terrorist, is extremely difficult. The greatest deterrent to cyber attacks should be the international community – with an agreed-upon code of conduct between states.

The Power of Cyberspace

> *In the years ahead, the Internet will have an even more profound effect on the way we work, live and learn. By enabling instantaneous and seamless communication and commerce around the globe, from almost any device imaginable, this technology will be one of the key cultural and economic forces of the early 21st century.*
>
> - Bill Gates[6]

For the United States, internet freedom and the ability to openly share information with others through cyberspace represents a way of life. As President Obama remarked in his State of the Union address in January 2011, American innovation is "how we make our living." The President also stated that his goal was to "...make it possible for businesses to deploy the next generation of high-speed wireless coverage to 98 percent of

all Americans" in the next five years.[7] Future advancement relies on cyberspace, not only in the U.S. but throughout the world. The wealthiest countries on the planet today are the primary beneficiaries of what cyberspace offers.[8] There is a digital divide throughout the world, but that is changing dramatically as more of the world gains access to the internet. In Africa alone, the use of the internet grew 1,392 percent from 2000 to 2009 with similar rates occurring in Asia, the Middle East, and Latin America.[9] Not all nations have access to the same high-speed connections the U.S. enjoys, but even a slow connection allows people to gather and send information. The most important aspect of cyberspace remains the information that resides within. Ultimately, the information that is stored, disseminated, processed, and shared across cyberspace is of vital importance.

The U.S. is increasing its efforts to promote internet freedom abroad – in developing countries and in counties that filter and screen much of what they allow their citizens to see on the internet. Congress allocated $30 million dollars of the fiscal 2010 budget to the State Department to help citizens "break through government firewalls in countries such as China and Iran."[10] Secretary of State Hillary Clinton has been a strong advocate for promoting internet freedoms. In a January 2010 speech, Secretary Clinton affirmed this commitment stating, "We stand for a single Internet where all of humanity has equal access to knowledge and ideas....and we recognize that the world's information infrastructure will become what we and other make of it."[11]

In the summer of 2006, the world watched as Lebanon turned into a battlefield between Hezbollah and Israel. Unlike any conventional war to which Israel had been accustomed, Hezbollah's most successful weapons of choice were the camera and computer.[12] One reporter described the events that unfolded over 34 days that summer as

a war that was "...broadcast via broadband. In places not accessible on the battlefield by car, a sole reporter with a laptop and small camera can shoot, edit, and do live interviews."[13] This allowed Hezbollah to broadcast its message of propaganda, showing Israel to be using a disproportionate amount of military force against "innocent civilians." Ultimately, Israel could not respond fast enough in the media to effectively counter the Hezbollah message, consequently losing the war at the strategic level.

Hezbollah won because it was able to dominate the "information battlefield," according to Steve Fondacaro, an American military expert.[14] Fondacaro goes on to explain that the struggle between Western modernity and Islamic fundamentalism will be resolved on this informational battlefield and that, "perception truly is reality, and our enemies know it."[15] Hezbollah and other terrorist organizations such as al-Qaeda fully understand that western democratic states with open societies can fall victim to this openness when it comes to the information battlefield. A closed organization such as Hezbollah can have total control and create a perception of legitimacy pertaining to its cause.[16] This is also the case for closed societies and countries that restrict internet access with government controls.

In certain parts of the world, specifically China and parts of the Middle East, the internet is not open. Some governments censor a great deal of information, both incoming and by curtailing what is said by its citizens. In fact, a Chinese official recently described the web as "fundamentally controllable."[17] Governments such as China, Iran, and North Korea will continue to control the internet and, in some instances, turn the internet off completely. The only way to overcome this government censorship will be by the will of its people, or when it becomes economically unbearable to continue

limiting the freedom of the internet, as we have seen in recent weeks with the uprisings across the Middle East.

In January 2011, anti-government protestors demanding more freedom and equality rose up in the small North African country of Tunisia. What followed was something that few people could have imagined. Longtime President Zine El Abidine Ben Ali fled Tunisia, and protests and unrest continued.[18] The successful ousting of Tunisia's corrupt leader was a spark plug for more anti-government protests that surged across the Middle East. Egypt, Yemen, Iran, Bahrain, Libya, and Morocco have erupted, joining the movement that started in Tunisia. These protests are extremely unique because of the manner in which they were organized – through the power of social media, particularly Facebook. In Yemen, a young woman by the name of Tawakkol Karman used her Facebook and cell phone text messages to get protestors to come out in force – culminating in some of the largest gatherings the nation has seen in recent times.[19]

Revolts in Egypt attracted the significant attention from around the world and, as in Yemen, the same social media outlets were responsible for helping to instigate the uprisings. The Egyptian government responded by shutting down the internet, trying to silence the voice of protest.[20] After a few days, the Egyptian government realized that the price had become too high, both economically and socially, and the internet was turned back on throughout the country.[21] Protests continued and Egyptian President Hosni Mubarak eventually stepped down from power.

Throughout the uprisings, specifically in the instances cited above, the power of cyberspace was shown to be real. The ability to share information and collaborate in real time is evident in the success of these anti-government protests. One of the Egyptian

protesters summed it up best when he said, "We would post a video on Facebook that would be shared by 60,000 people on their walls within a few hours. I've always said that if you want to liberate a society, just give them the Internet."[22]

Shutting off the internet is not an option, and one the U.S. should never advocate. As stated earlier, cyberspace is a growing commodity and it does not take high-speed connections to be effective. As capacity increases, here at home and abroad, the power of cyberspace and the freedoms it presents to those around the world will continue to rise in dramatic fashion. However, the same conduit that provides the ability to share information, presents an opportunity for those that wish to do harm to others – cyber criminals and hackers.

Cyberspace Threats

> *Enemies in the future, however, need not destroy our aircraft, ships, or tanks to reduce our conventional and even nuclear effectiveness. A well-timed and executed cyber attack may prove just as severe and destructive as a conventional attack.*
>
> - General James N. Mattis [23]

Frederick the Great once said, "He who defends everything defends nothing."[24] This is very true in military tactics on the battlefield; however, in cyberspace, one must defend everything to secure both information and critical infrastructure. In 2007, a computer security company, McAfee, conducted a study on the number of countries engaging in research on how to use the internet for war-fighting purposes. It found over 120 countries trying to develop technologies to leverage the internet for war.[25] This research is not just theoretical, as the following cases illustrate.

In 2000, Estonia's Parliament declared online access a human right and established the small country as "one of the world's most wired countries."[26] In late

April 2007, a denial of service attack took place in Estonia, crippling the banking system, media outlets, and government ministries for days.[27] Although the attack did not cause any physical damage, the access-related problems and redirected web pages (some links redirected users to iconic Soviet soldiers and quotations from Martin Luther King Jr. about fighting evil) caused frustration among users.[28] This assault was denounced, and Estonia publicly blamed Russia for carrying out the attacks. A year later, after Russia invaded the small country of Georgia, Russia was blamed again for another denial of service attack against Georgia. Users were denied access and, in some instances, redirected altogether to other websites.[29] Russia again denied responsibility for the attacks.

From May 2007 to March of 2009, cyber attacks called "GhostNet" attacks occurred globally, infiltrating at least 1,295 computers in 103 different countries.[30] Unlike the attacks in Estonia and Georgia that were mere disruption of services, these attacks were carried out to retrieve sensitive information using a combination of phishing and malware strategies.[31] Many blamed China for the attacks. Like Russia, the Chinese publicly denied the claims and redirected the blame back on citizens in the countries that were affected – the "rogue citizen" defense. An official from the Chinese government claimed, "I will not be surprised if this report is just another case of their recent media propaganda campaign."[32]More recently, Canada's Finance Department and Treasury Board – key economic ministries – were hacked, forcing the Canadian government to shut those respective ministries off from the internet for a period of time.[33] The attacks were carried out in similar fashion to the "GhostNet" attacks, and Canada blamed Chinese hackers.

In June 2007, the U.S government blamed the Chinese for hacking into the U.S Departments of State, Commerce, and Defense, making off with some data and, in the instance of the DoD, actually shutting down a small portion of the network for a short while in the Pentagon.[34] The Chinese are the most active in cyberspace in terms of probing its adversaries' networks. However, China regularly denies state involvement, claiming rogue citizens are the culprits, rather than the Chinese government.

Probably the most malicious cyber attack to take place within the last year was a worm called Stuxnet, a form of malware – malicious software – that caused a considerable setback to the Iranian nuclear program.[35] Stuxnet was introduced into cyberspace at an unknown origin, slowly spreading across the digital domain. It exploited computers running Microsoft Windows operating systems, specifically searching for software created by German engineering company Siemens for use in power plants and factories.[36] Once malware finds its intended target, it makes modifications to the machinery to shut it down or perform widely out of control. In the case with Stuxnet, the worm not only caused disruption to the machines in the nuclear power plant, it also fooled the feedback software so engineers had no idea what was really happening.[37] For most users, there were no side effects to Stuxnet. However, to nuclear power plants in Iran running Siemens, the results were catastrophic, possibly setting them back two years in full development of a nuclear weapon. However, recent news coverage on Stuxnet revealed that Iran was able to recover swiftly and Washington, D.C based nuclear experts concluded that the net impact was minor.[38] Some experts believe that this act was one of a very powerful nation, such as Israel or the United States,

because of the sophistication in the malware. As with the other instances, no nation has acknowledged any wrongdoing in the matter.

In February 2011, hackers infiltrated the NASDAQ communications service in the U.S. that handles confidential communications for some 300 corporations.[39] The target of the attack was a service called Director Desk, which helps companies share documents between directors at scheduled board meetings.[40] Board directors have access to information at the highest levels and any intrusion on this data by an outsider could have great value for insider trading. Unlike the previous examples, the inquiry is still underway with no suspected culprit yet identified.

The examples show not only the sophistication of what is possible, but also how difficult it is to defend against and ultimately hold those responsible accountable. Are the attacks actions of a few rogue citizens or are they coordinated government cyber attacks? Someone or something must be held accountable for these actions. In the instance of the NASDAQ hacking, this could have been done by someone here in the U.S. If this is the case, this situation is potentially easier to handle in the judicial system of the U.S. Of greater debate: Should the U.S. government treat a state actor differently than a non-state actor or rogue individual committing cyber attacks and infiltration?

Attribution: State vs. Non-State

> *"We will pursue nations that provide aid or safe haven to terrorism. Every nation, in every region, now has a decision to make. Either you are with us, or you are with the terrorists. From this day forward, any nation that continues to harbor or support terrorism will be regarded by the United States as a hostile regime."*
>
> -President Bush[41]

Delivering his presidential speech to a joint session of Congress and the nation days after 9/11, President Bush made his famous comments, "either you are with us, or you are with the terrorists."[42] His remarks were directed at other countries supporting terrorist regimes and their ruthless networks, hiding and harboring terrorists within their national boundaries. The "Bush doctrine," as it came to be known, posited that the U.S. would make no distinction between the individual terrorist and the government he hides behind. It also argued that preemptive unilateral action could be taken when national security interests were at stake. The Bush doctrine is a model for the U.S. government to follow when dealing with countering cyber attacks and espionage in cyberspace.

The attack against Estonia described earlier was declared a "pre-emptive digital strike" which could not be "treated as hooliganism...but as an attack against the State," according to Estonia's Defense Minister.[43] Blame for the cyber attacks in Estonia and the GhostNet attacks was laid on the governments of Russia and China, respectively. So what is the U.S. to do when a cyber attack occurs against either the private sector or the military and the suspected culprit is another nation state? In 2004, a high-level Pentagon panel claimed that in an event of a cyber attack on the U.S., the use of nuclear weapons should be a consideration.[44] However, in the 2010 U.S. nuclear strategy, nuclear retaliation in response to a cyber attack was ruled out. Interestingly enough, however, the U.S. nuclear strategy does delineate exceptions for certain states, including Iran and North Korea.[45]

It is outrageous to think that the U.S. would consider a nuclear strike of any kind in response to a cyber attack, regardless of any nation considered to be behind it. A military strike should only be considered when military actions are already being

conducted against the nation responsible for a cyber attack. The cyber attacks on Georgia in 2008 are considered "cyber warfare" because they were accompanied by a military offensive.[46] Cyber warfare by the U.S. should only be conducted in concert with ongoing military operations, except for certain states like our nuclear strategy. Cyber attacks will continue to resemble an early chess match - a pawn for a pawn, rarely trying to go after the King upfront. Retaliation should come in the form of a like attack, where eventually both sides see that there is no productive outcome to the cyber attacks and ultimately neither side chooses to engage in the matter further.

The harder question is what to do about the non-state actor or rogue individual who is responsible for a cyber attack against the U.S. In all of the cases presented earlier, not one nation took the blame and outwardly admitted to conducting the cyber attack. Each put the blame on a rogue citizen that "hijacked" the internet within the state to make it look like the government was responsible. Plausible deniability was another acceptable defense, as was the case with the Stuxnet worm on the Iranian nuclear facility.

As U.S. Deputy Defense Secretary William J. Lynn III stated, "Deterrence is predicated on the assumption that you know the identity of your adversary, but that is rarely the case in cyberspace, where it is so easy for an attacker to hide."[47] No return address for individuals, groups, or states committing cyber attacks makes it hard to track down who is truly responsible.[48] Locating the origin of a cyber attack and building concrete proof of guilt is extremely difficult. This is especially the case with a cyber attack that occurred in July of 2009 when "zombie" computers from 16 different countries from around the globe inadvertently participated in the cyber attack.[49] An investigator for Information Warfare Monitor, Rafal Rohozinski noted, "Attribution is

difficult because there is no agreed upon international legal framework for being able to pursue investigations down to their logical conclusion, which is highly local."[50]

On the contrary, the U.S. does possess the technological edge to pinpoint origins of cyber attacks in most cases. Because of this, the Bush doctrine should be applied and ensure that the nation from which the cyber attack originated is held accountable. There should be no delineation between a state and non-state actor. James Lewis is Director of the Center for Strategic and International Studies (CSIS) Technology and Public Policy Program, a program that looks at technological development and how that affects security and economic growth.[51] He openly disputes that countries such as Russia and China cannot stop cyber attacks from being executed within its national territories. Lewis argues that many of the countries which are "havens for cyber crime have invested billions in domestic communications monitoring to supplement an already extensive set of police tools for political control."[52] Lewis finds it difficult to accept "the notion that a cybercriminal in one of these countries operates without the knowledge and thus tacit consent of the government."[53]

U.S. networks are probed every day for vulnerabilities, sometimes by very powerful nation states, and other times by amateur hackers wanting to see how far they can take it before getting caught. Most of these intrusions are to gain information on sensitive information both from the private sector and in the military. Does probing the network constitute a retaliatory act? U.S. reactions to this point say no. Amateur hackers are not as large of a concern. Rather, the U.S. must address the world class expert with the ability to hide his steps and ultimately put blame on others for his actions, whether an individual or state. Curtailing cyber attacks in the international cyber community will

rely on good deterrence and – more importantly – the kind of international policies put in place in the future.

Cyberspace Deterrence and Policy

> *"To maintain an Internet that delivers the greatest possible benefits to the world, we need to have a serious conversation about the principles that will guide us."*
>
> -Secretary Hillary Clinton[54]

Deterrence alone will not be enough to prevent cyber attacks from occurring between nation states, and certainly between a nation and a non-nation entity. There needs to be sound policy governing the way countries utilize cyberspace. Though the U.S. views cyberspace as a national security issue, the development of a cyber warfare strategy must reside at the international level. A "one state, one mind" approach will not be sufficient if the U.S. truly wants cyber deterrence to be an option.[55] Deterrence and policy must go hand in hand to be successful, with the world community coming together to have an open discussion about the future of cyberspace and how it pertains to warfare.

There are treaties and accords in existence that provide a start point to begin discussions on regulating cyber attacks and espionage in cyberspace. Such examples are the Chemical Weapons Convention, Nuclear Non-Proliferation Treaty (NPT), and parts of the Bush doctrine as mentioned earlier.[56] Parallel lines can be drawn between piracy and cyber crimes. Because piracy does not have any recognized geographic borders, it is considered an international crime where the concept of "universal jurisdiction" applies. Under that rule, any country can capture and punish a pirate on the high seas. The concept of universal jurisdiction may provide the foundation for open and truthful communication about cyber warfare and what that may mean to future generations. The

NPT, signed by 189 countries since July of 1968, provides the most substantial evidence to date that establishing sound international policy towards cyberspace is possible.[57] What is unique in the NPT is that it deals with both nuclear states and non nuclear states – just as we have to identify the difference in cyber attacks from rogue individuals or the actual state itself.

Certainly, barriers exist to achieving an NPT-like cyber document to provide sound deterrence against cyber attacks and intrusions. In fact, the U.S. government is one of the biggest barriers to its development. The great deal of secrecy that goes into cyberspace related policymaking precludes open discussion, especially with the U.S. Many analysts from other countries note the U.S.'s hypocrisy when it comes to criticizing the stealth of cyber warfare policies by the likes of Russia and China, while remaining incredibly secretive about its own policy and actions in cyberspace.[58] However, as Marcus Sachs, one of the founders of the first cyberwarfare units in the U.S., so eloquently put it, "we need to have a public debate, not a classified conversation"[59] when it comes to devising policy on cyberspace.

While there is hope for a policy to be put in place by the international community to deter aggressors from conducting possibly devastating cyber attacks, there are significant hurdles to accomplishing the task. Every nation and society throughout the world is different, and can see the same actions but react differently. Cyberspace is no exception. The lexicon on what constitutes a cyber attack is different from state to state. Where one state may see a cyber attack as an act of war, such as Estonia's reaction when attacked in 2007, another state may see the same attack along the lines of vandalism.[60] A universally agreed-upon cyber lexicon is inherent to a successful strategy at the

international level. The U.S. cannot have a different playbook from other countries, such as Russia and China. James Lewis clarifies the implications of cyber security in regards to a national versus international problem best by saying:

> We have, at best, a few years...to modernize our laws to allow for adequate security...The United States will need to define doctrine for the use of the cyber attack as a tool of national power. It would benefit from an effort to reshape the international environment for cyber conflict in ways that could reduce risk, to win consensus (as we did with proliferation) on a set of norms and constraints for cyber conflict.[61]

The U.S. is taking measures to look into doctrine and how best to use cyber attack as a national power, along the lines of military power. With the recent establishment of U.S. Cyber Command (USCYBERCOM), it seems that the U.S. is serious about not only securing vital interests in cyberspace, but also looking to go on the offensive when it seems appropriate to do so.

Department of Homeland Security & USCYBERCOM

> *Information technology provides us with critical advantages in all of our warfighting domains so we need to protect Cyberspace to enable those advantages.*
>
> -Deputy Defense Secretary William J. Lynn III[62]

The Department of Homeland Security (DHS) was created in 2002 by President Bush to unite 22 federal agencies in the common purpose of improving homeland security in wake of the 9/11 attacks.[63] DHS is the lead department for the President when in comes to responsibilities in cyberspace security, which include: developing a comprehensive national plan to secure key resources, such as critical infrastructure; providing crisis management in response to attacks; providing technical response to private sector and other government agencies in respect to emergency recovery plans;

coordinating with other agencies of the federal government to provide specific warning information and advice about appropriate protective measures and countermeasures to state, local, and nongovernmental organizations; and funding research and development along with other agencies that lead to new scientific understanding.[64] DHS is a critical player when it comes to leading the government and private sector in cyber defense for the nation. DHS looks to United States Cyber Command (USCYBERCOM) for assistance when it comes to taking the initiative on and exploiting possible cyber attacks.

USCYBERCOM, located at Fort Meade, Maryland, was officially established in May 2010. It is a sub-unified command of U.S Strategic Command (STRATCOM), a functional combatant commander (COCOM). Unique to USCYBERCOM is that the commander commands both USCYBERCOM and the National Security Agency (NSA). This dual command is in place because the NSA currently has a huge role operating in cyberspace. Cyber attacks on various countries' infrastructures in recent years spurred the need within the Department of Defense (DoD) to create a specific command to counter very real threats in cyberspace. With USCYBERCOM established, DoD has acknowledged that it is taking the next step in adding "cyberspace" to land, sea, air, and space as the latest domain in warfare.[65]

As the U.S. military looks at how it conducts business on the battlefield today and in the future, cyberspace should be the driving force to all other actions taken in the domains listed above. The U.S.'s Intelligence, Surveillance, and Reconnaissance (ISR) community is very dependent on the health of cyberspace. Air Force General Robert Elder commented, "When we talk about the speed, range, and flexibility of air power, the thing that enables this for us is the fact of our cyber-dominance."[66] It is critical that the

military not only effectively operate within the domain for intelligence and continued air power dominance, but even more so that it is protected. Without mastery of our computerized technology, many of our weapon systems and Command and Control (C2) systems will not work.[67] The Global Information Grid (GIG), the military's communication backbone, consisting of 15,000 networks and 7 million computing devices across hundreds of installations in dozens of countries, becomes a very enticing target for our adversaries and must be defended.[68]

The challenges are very real as USCYBERCOM continues to develop its roles and responsibilities in cyberspace. Currently, the three core missions outlined for USCYBERCOM are: to lead the day-to-day defense of the .mil networks, support military and counterterrorism missions, and under the leadership of DHS, assist civil authorities and industry partners.[69] "The National Strategy To Secure Cyberspace," is the guiding overarching document for the Department of Homeland Security (DHS) in the overall effort to protect our nation.[70] Recently, the Obama administration instituted a change in federal policy, allowing for military involvement and assistance to DHS if a cyber attack is carried out on domestic soil. The memorandum signed by DHS Secretary Janet Napolitano and DOD Secretary Robert Gates, signifies the importance of cyberspace to this Nation and to those around the world.

As cyberspace continues to grow in its availability and complexity, the role that USCYBERCOM plays will be pivotal not only within the DoD, but to all other government agencies and the country's private sector as well. In fact, the private sector may have more prestigious targets than the government, for economic reasons. For example, it is estimated that shutting down a power grid in any sizable region for more

than ten days would stop over 70 percent of all economic activity in that region.[71] If an attack on critical infrastructure such as the power grid can provide those sorts of results, why would an adversary even consider a traditional military attack? The 2011 DoD budget calls for $2.3 billion dollars to go toward cyber security, a significant show of economic force to bolster the U.S.'s efforts in cyberspace.[72] This will not only help in USCYBERCOM's mission, but will enhance its ability to assist the private sector in protecting vital interests, such as critical infrastructure and telecommunications networks throughout the country.

Conclusion

> *The world of cyber-crime, cyber terrorism, and cyber warfare is truly a wild, unruly, and ungoverned place.*
> -David Tohn[73]

The accelerated pace of change and the endless possibilities that cyberspace has given to the world is here to stay. If social media can organize protestors to rise up in support of freedom, it should be embraced by the U.S. and all nations that support democracies throughout the world. When discussions are held relating to internet freedoms, the next question that will always arise is one of security. The two cannot be separated, and an appropriate balance should be found – especially for the U.S. government.

On a micro-level analysis when it comes to security, everyone plays an active role in a nation's security. The best way to hack a network is from within the network itself; this is why phishing techniques are so numerous. Best practices such as good password protection and ensuring that an email one opens is from a trusted source are very basic practices, yet very effective in the defense in-depth approach. As stated earlier, the

information in cyberspace is of critical importance for all users – whether it be military secrets or personal information such as a social security number. Developing new technologies that encrypt the actual data will be important in the coming years. Ensuring that confidential data is seen by only the appropriate required individuals adds another level of complexity for the would-be cyber hacker.

The U.S. fully understands that a loss of cyberspace dominance could be devastating to U.S. interests. In February 2008, Director of National Intelligence Michael McConnell discussed "cyber threats" before talking about the war in Afghanistan in his annual threat assessment delivered to Congress.[74] Considering that the Afghanistan war is the number one priority for U.S. interests abroad, McConnell's attention to cyber threats demonstrated that top U.S. government leaders view cyberspace as critical to national interests. True deterrence must come with the cooperation of the international community; it cannot be the U.S. government doing it alone.

The structure of the NPT offers great insight on how to possibly achieve a cyber warfare international treaty, but the Bush doctrine offers up the best approach to combating cyber crimes. While many U.S. foreign policy experts and historians have criticized the "you're either with us or against us" part of the Bush doctrine as a radical departure from previous international law, it seems to have been accepted over the years by many other key international players, such as Russia and Israel.[75] If other nations have utilized it as part of their doctrine on how to handle certain political situations, then there is hope that it could be used for discussions on cyberspace deterrence at the international level.

DHS and USCYBERCOM will continue to develop leading edge technologies and policies that will help defend our critical nodes throughout the country – both government and private sectors. The good news for now is, most cyber attacks to date have been relatively minor setbacks. This is the case with the Stuxnet incident, causing only a minor setback. The denial of service attacks in Estonia was purely nuances' to public and government services.

These are revolutionary times, and much like an iceberg, we have only seen above the surface as it relates to cyberspace and its impact on not only societies but how it will impact warfare for today and tomorrow. It is not inconceivable to think that probing networks and small scale denial of service attacks will continue to grow in numbers, and continue to be denied with no public acknowledgment on either side. An international agreement on cyberspace security, with widely acceptable norms and procedures for cyber warfare, would do a few things.[76] It would deter cyber attacks, because it would make such attacks seem less tantalizing. It would create an incentive to preemptively detect, target, and neutralize non-state actors attempting to carry out attacks within a nation's territory, instead of turning a blind eye and putting blame on the "rogue citizen." Finally, and probably most importantly, an agreement would provide a forum for nations to discuss their disputes openly. If the world is going to balance internet freedom with security, such an agreement must exist.

Endnotes

[1] P.W. Singer. Wired for War: The Robotics Revolution and Conflict in the 21st Century. The Penguin Press: New York, NY, 2009. Pg 19.

[2] USMC Cyberspace Concept. Marine Corps Combat Development Command. MCB Quantico, VA, 2009.

[3] Ibid.

[4] http://wiki.answers.com/Q/How_many_web_sites_are_there_in_the_World_Wide_Web. January 16, 2011.

[5] The White House. The National Strategy to Secure Cyberspace. Washington, DC 2003. Pg 1.

[6] Bill Gates. Shaping the Internet Age. Internet Policy Institute, 2010. http://www.microsoft.com/presspass/exec/billg/writing/shapingtheinternet.mspx. January 15, 2011.

[7] "Transcript: Obama's State of the Union Address." National Public Radio. January 25, 2011.

[8] Daniel Ventre. Information Warfare. John Wiley & Sons, Inc. Hoboken, NJ. 2009. Pg 23.

[9] Dennis M. Murphy. "Attack or Defend? Leveraging Information and Balancing Risk in Cyberspace." Military Review. 2010. Pg 90.

[10] Mary Beth Sheridan. "Clinton warns other nations: Blocking Internet will backfire." The Washington Post. February 16, 2011.

[11] "The fight for Internet freedom." The Washington Post. February 6, 2011.

[12] Marvin Kalb. "The Israeli-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict." KSG Faculty Research Working Paper Series, John F. Kennedy School of Government, Harvard University, February 2007. Pg 4.

[13] Ibid, Pg 23.

[14] Ibid, Pg 6.

[15] Ibid.

[16] Ibid, Pg 5.

[17] "The fight for Internet freedom."

[18] Sudarsan Raghavan. "Defying obstacles, a female activist presses for reform." The Washington Post. February 15, 2011.

[19] Ibid.

[20] "The fight for Internet freedom."

[21] "The fight for Internet freedom."

[22] Jeffrey Ghannam. "Freedom, beyond 140 characters." The Washington Post. February 20, 2011

[23] Marine Corps Combat Development Command. USMC Cyberspace Concept.

[24] http://thinkexist.com/quotes/frederick_the_great/. February 20, 2011.

[25] Ryan T. Kaminski. "Escaping the Cyber State of nature: Cyber Deterrence and International Institutions." Conference on Cyber Conflict Proceedings 2010. Columbia University, NY, USA. Pg 80.

[26] Ibid, Pg 81.

[27] Greg Bruno. The Evolution of Cyber Warfare. Council on Foreign Relations, 2008.

[28] Kaminski, Pg 81.

[29] Ibid, Pg 82.

[30] Ibid.

[31] Ibid.

[32] Ibid, Pg 83.

[33] John Leyden. "Canadian finance ministries closed off from the web after cyberspy hack: Blame ~~Canada~~ China." The Register. February 17, 2011.

[34] Greg Bruno. The Evolution of Cyber Warfare. Council on Foreign Relations, February 27, 2008.

[35] Barry Neild. "Does Stuxnet herald the age of cyber warfare?" Global Post, October 18, 2010.

[36] Barry Neild.

[37] Ibid.

[38] Joby Warrick. "Iran recovered swiftly in wake of cyberattack." The Washington Post. February 16, 2011.

[39] Peter Svensson. "Hackers infiltrate Nasdaq communications service; inquiry underway." The Washington Post. February 6, 2011.

[40] Ibid.

[41] "President Bush's address to a joint session of Congress and the nation." The Washington Post. September 20, 2001.

[42] Ibid.

[43] Kaminski, Pg 84.

[44] Kaminski, Pg 85.

[45] Ibid.

[46] Ibid.

[47] Ibid, Pg 86.

[48] Ibid, Pg 80.

[49] Ibid, Pg 86.

[50] Ibid.

[51] "Technology and Public Policy Program." Center for Strategic and International Studies. http://csis.org/program/technology-and-public-policy. Pg 1.

[52] Ibid, Pg 86.

[53] Ibid, Pg 86.

[54] Sheridan.

[55] Ibid, Pg 88.

[56] Sheridan, Pg 81.

[57] "Technology and Public Policy Program," Pg 90.

[58] Ibid, Pg 87.

[59] Ibid.

[60] Ibid, Pg 84.

[61] Ibid, Pg 89.

[62] Cheryl Pellerin. Lynn: Cyberspace is the New Domain of Warfare. American Forces Press Service, October 18, 2010. http://www.defense.gov/news/newsarticle.aspx?id =61310. January 22, 2011.

[63] "The National Strategy to Secure Cyberspace." The White House. Washington, DC 2003.

[64] The White House. The National Strategy to Secure Cyberspace. Washington, D.C., 2003.

[65] Ibid.

[66] Bruno.

[67] Marine Corps Combat Development Command. USMC Cyberspace Concept. Pg 1.

[68] Pellerin.

[69] William J. Lynn III. "Remarks at Stratcom Cyber Symposium." U.S. Department of Defense. Deputy Secretary of Defense William J. Lynn III. Omaha, NE. May 26, 2010.

[70] The White House. The National Strategy to Secure Cyberspace. Washington, D.C., 2003.

[71] Bruno.

[72] Walter Pincus. "Winners and Losers." The Washington Post. February 15, 2011.

[73] Kaminski, Pg 80.

[74] Bruno.

[75] Kaminski, Pg 91.

[76] Kaminski, Pg 92.

Bibliography

Alberts, David S., John J. Garstka, Richard E. Hayes, and David T. Signori. Understanding Information Age Warfare. DoD Command and Control Research Program. Washington, D.C 2004.

Art, Robert J. and Robert Jervis. International Politics; Enduring Concepts and Contemporary Issues. Eighth Edition. Pearson Education, New York 2007.

Bartholomees, J. Boone, Jr. U.S. Army War College Guide to National Security Issues; Volume II: National Security Policy and Strategy. Department of National Security and Strategy. 2008.

Bush, George W. Decision Points. Crown Publishers; New York, NY 2010.

Broad, William J., John Markoff, and David E. Sanger. "Israeli test on Worm Called Crucial in Iran Nuclear Delay." The New York Times, January 16, 2011.

Bruno, Greg. "The Evolution of Cyber Warfare." Council on Foreign Relations. February 27, 2008. http://www.cfr.org/publication/15577/evolution_of_cyber warfare.html. February 19, 2011.

Clausewitz, Carl Von. On War. Princeton University Press; Princeton University, NJ 1976.

Czosseck, Christian and Geers, Kenneth. The Virtual Battlefield: Perspectives on Cyber Warfare. IOS Press, Washington, DC. 2009.

"Technology and Public Policy Program." Center for Strategic and International Studies. http://csis.org/program/technology-and-public-policy. March 27, 2011.

Derfler, Frank J. Jr. and Les Freed. How Networks Work, Fourth Edition. Macmillan Computer Publishing/Que Corporation; Indianapolis, Indiana 1998.

"Fight for Internet freedom." The Washington Post. February 6, 2011.

Gates, Bill. "Shaping the Internet Age." Internet Policy Institute, 2010. http://www.microsoft.com/presspass/exec/billg/writing/shapingtheinternet.mspx

Gray, Colin S. Another Bloody Century; Future Warfare. Weidenfeld & Nicolson, The Orion Publishing Group Ltd. London, United Kingdom 2005.

Grossman, Lev. "2045: "The Year Man Becomes Immortal." Time Magazine. February 21, 2011.

Grund, William C. and Joseph H. Scherrer. A Cyberspace Command and Control Model. Air War College Maxwell Paper, No. 47. Maxwell Air Force Base, Alabama 2009.

Hedgpeth, Dana. "WikiLeaks, Free Speech and Twitter." The Washington Post. February 16, 2011.

"How Many Web Sites Are There in the World Wide Web?" January 16, 2011. http://wiki.answers.com/Q/How many web sites are there in the World Wide Web. January 16, 2011.

http://thinkexist.com/quotes/frederick_the_great/. February 20, 2011.

Joint Tactics, Techniques, and Procedures for Tactical Lateral Links. Joint Mobile Network Operations, Joint Test and Evaluation. MCB Quantico, VA 2009.

Ghannam, Jeffrey. "Freedom, beyond 140 characters." The Washington Post. February 20, 2011.

Kaminski, Ryan T. "Escaping the Cyber State of Nature: Cyber Deterrence and International Institutions." Conference on Cyber Conflict Proceedings 2010. Columbia University, New York, USA, 2010.

Leyden, John. "Canadian finance ministries closed off from the web after cyberspy hack: Blame ~~Canada~~ China." The Register. February 17, 2011. http://www.theregister.co.uk /2011/02/17/canada_cyber_espionage/. February 20, 2011.

Libicki, Martin C. Conquest in Cyberspace; National Security and Information Warfare. Cambridge University Press; New York, NY. 2007.

Libicki, Martin C. Defending Cyberspace and other Metaphors. The Center for Advanced Concepts and Technology. National Defense University. Washington, D.C., 1997.

Libicki, Martin C. What is Information Warfare? The Center for Advanced Concepts and Technology. National Defense University. Washington, D.C., 1995.

Loshin, Pete. TCP/IP Clearly Explained. Academic Press. San Diego, CA, 1997.

Lynn, William J., III. "Remarks at Stratcom Cyber Symposium." U.S. Department of Defense. Deputy Secretary of Defense William J. Lynn III. Omaha, NE. May 26, 2010. http://www.defense.gov/speeches/speech.aspx?speechid=1477. January 22, 2011.

MCDP-6 Command and Control. United States Government, Secretary of the Navy. Arlington, VA, 1996.

Marine Corps Operating Concepts. Marine Corps Combat Development Command. MCB Quantico, VA, 2010.

Kalb, Marvin. "The Israeli-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict." KSG Faculty Research Working Paper Series, John F. Kennedy School of Government, Harvard University, February 2007.

Molander, Roger C., Andrew S. Riddile, and Peter A. Wilson. Strategic Information Warfare; A New Face of War. National Defense Research Institute, CA, 1996.

Murphy, Dennis M. "Attack or Defend? Leveraging Information and Balancing Risk in Cyberspace." Military Review. 2010.

"National Strategy to Secure Cyberspace." The White House. Washington, DC 2003.

Neild, Barry. "Does Stuxnet herald the age of cyber warfare?" Global Post. October 18, 2010.

Pellerin, Cheryl. "Lynn: Cyberspace is the New Domain of Warfare." American Forces Press Service, October 18, 2010. http://www.defense.gov/news/newsarticle.aspx?id=61310

Pincus, Walter. "Winners and Losers." The Washington Post. February 15, 2011.

"President Bush's address to a joint session of Congress and the nation." The Washington Post. September 20, 2001.

Raghavan, Sudarsan. "Defying obstacles, a female activist presses for reform." The Washington Post. February 15, 2011.

Rashid, Fahmida. "Pentagon to Help Homeland Security Fight Cyber-attacks on U.S. Soil." Government & Federal IT Technology News, 2010. http://www.eweek.com/c/a/Government-IT/Pentagon-to-Help-Homeland-Security-Fight-CyberAttacks-on-US-Soil-862923/

Sheridan, Mary Beth. "Clinton warns other nations: Blocking Internet will backfire." The Washington Post. February 16, 2011.

Singer, P.W. Wired for War: The Robotics Revolution and Conflict in the 21st Century. The Penguin Press; New York, NY 2009.

Sutter, John D. "The faces of Egypt's 'Revolution 2.0'." CNN. February 21, 2011. http://www.cnn.com/2011/TECH/innovation/02/21/egypt.internet.revolution/index.html?hpt=C1#

Svensson, Peter. "Hackers infiltrate Nasdaq communications service; inquiry underway." The Washington Post. February 6, 2011.

"Transcript: Obama's State of the Union Address." National Public Radio. January 25, 2011. http://www.npr.org/2011/01/26/133224933/transcript-obamas-state-of-union-address. March 27, 2011.

"Understanding Cyberspace as a Medium for Radicalization and Counter-Radicalization." Hearing before the Terrorism, Unconventional threats and Capabilities Subcommittee of the Committee on Armed Services House of Representatives, One Hundred Eleventh Congress, First Session, held on December 16, 2009. U.S Government Printing Office, Washington, D.C., 2010.

USMC Cyberspace Concept. Marine Corps Combat Development Command. MCB Quantico, VA, 2009.

U.S. Marine Corps Concepts & Programs 2010. Programs Assessment and Evaluation Division. Arlington, VA, 2010.

Ventre, Daniel. Information Warfare. John Wiley & Sons, Inc. Hoboken, NJ, 2009.

Warrick, Joby. "Iran recovered swiftly in wake of cyberattack." The Washington Post. February 16, 2011.